A Note on "On the Construction of Boolean Functions with Optimal Algebraic Immunity"

Yuan Li, Haibin Kan *and Futatsugi Kokichi†

Abstract

In this note, we go further on the "basis exchange" idea presented in [2] by using Mobious inversion. We show that the matrix $S_1(f)S_0(f)^{-1}$ has a nice form when f is chosen to be the majority function, where $S_1(f)$ is the matrix with row vectors $\upsilon_k(\alpha)$ for all $\alpha \in 1_f$ and $S_0(f) = S_1(f \oplus 1)$. And an exact counting for Boolean functions with maximum algebraic immunity by exchanging one point in on-set with one point in off-set of the majority function is given. Furthermore, we present a necessary condition according to weight distribution for Boolean functions to achieve algebraic immunity not less than a given number.

Index Terms-algebraic attacks, algebraic degree, algebraic immunity, Boolean functions.

1 Introduction

Let $\mathcal{F}_2$ be the finite field with only two elements. To prevent confusion with the usual sum, the sum over $\mathcal{F}_2$ is denoted by $\oplus$. The Hamming weight of a vector $\alpha = (\alpha_1, \ldots, \alpha_n)$ is defined by $\mathrm{wt}(\alpha) = \sum_{i=1}^{n} \alpha_i$.

A Boolean function on n variables may be viewed as a mapping from $\mathcal{F}_2^n$ into $\mathcal{F}_2$. We denote by $\mathcal{B}_n$ the set of all n-variable Boolean functions. The Hamming weight $\mathrm{wt}(f)$ is the size of the support $\mathrm{supp}(f) = \{x \in \mathcal{F}_2^n \mid f(x) = 1\}$. The support of f is also called the on set of f, which is denoted by 1_f. On the contrary, the off set of f is the set $\{x \in \mathcal{F}_2^n \mid f(x) = 0\}$, which is denoted by 0_f. Any $f \in \mathcal{B}_n$ can be uniquely represented as

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{\alpha \in \mathcal{F}_2^n} c_\alpha \prod_{i=1}^{n} x_i^{\alpha_i} = \bigoplus_{\alpha \in \mathcal{F}_2^n} c_\alpha x^\alpha, \tag{1}$$

This kind of expression of f is called the Algebraic Normal Form(ANF). The algebraic degree of f is the number of variables in the highest order term with nonzero coefficient, which is denoted by $\deg(f)$.

For $f, g \in \mathcal{B}_n$ and $g \neq 0$, g is called an annihilator of f if $f \cdot g = 0$. The algebraic immunity(AI) [8] of f is defined to be the minimum degree of an annihilator of f or $f \oplus 1$. It's proved [9] that the algebraic immunity of functions in $\mathcal{B}_n$ is upper bounded by $\lceil \frac{n}{2} \rceil$.

*Computer Science Department, Fudan University. Email:hbkan@fudan.edu.cn

†Graduate School of Information Science, JAIST (Japan Advanced Institute of Science and Technology). Email:kokichi@jaist.ac.jp

A majority function f in $\mathcal{B}_{2k-1}$ or $\mathcal{B}_{2k}$ is defined as

$$f(\alpha) = \begin{cases} 0, & \mathrm{wt}(\alpha) < k, \\ 1, & \mathrm{wt}(\alpha) \geq k. \end{cases}$$

It's well-known that $AI(f) = k$, which achieves the maximum.

In linear space $\mathcal{F}_2^n$, we define a partial order "$\preceq$" as follows. For $\alpha, \beta \in \mathcal{F}_2^n$, $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$, $\alpha \preceq \beta$ if and only if $\alpha_i \leq \beta_i$ for all $1 \leq i \leq n$. Similarly, for two nonnegative integers a and b with binary representation $(a_n, \ldots, a_0)_2$, $(b_n, \ldots, b_0)_2$ respectively, we define $a \preceq b$ if and only if $a_i \leq b_i$ holds for all $0 \leq i \leq n$. Furthermore, we define $a \wedge b = (a_n b_n, \ldots, a_0 b_0)$. In other words, $a \wedge b$ is the common greatest lower bound over a lattice induced by partial order "$\preceq$" on integers.

Throughout this paper, we use we use $\binom{n}{m}$ to denote the binomial coefficient and $\begin{bmatrix} n \\ k \end{bmatrix}$ to denote its module 2, i.e., $\begin{bmatrix} n \\ k \end{bmatrix}$ could be viewed as the value of $\binom{n}{m}$ over $\mathcal{F}_2$.

It's easy to prove that $\begin{bmatrix} n \\ k \end{bmatrix} = 1$ if and only if $m \preceq n$. And equation

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} \lfloor \frac{n}{q} \rfloor \\ \lfloor \frac{n}{q} \rfloor \end{bmatrix} \begin{bmatrix} n \mod q \\ m \mod q \end{bmatrix}$$

holds if positive integer q is a power of 2.

For any matrix $A \in \mathcal{F}_2(n \times m)$, denote by A^T the transpose of A. Denote by

$$A(i_1, i_2, \ldots, i_p; j_1, j_2, \ldots, j_q) \text{ and } A(j_1, j_2, \ldots, j_q)$$

the submatrix consisting of the i_1th, i_2th, ..., i_pth rows and the j_1th, j_2th, ..., j_qth columns of A and the submatrix consisting of the j_1th, j_2th, ..., j_qth columns of A. We use $A(i, j)$ for the (i, j) element of the matrix A. Sometimes the rows and columns of a matrix are indexed by vectors. Sometimes the rows and columns are indexed by integers starting from 1.

Following is a lemma which will be used in the sequel.

Lemma 1.1. *[1] Let S be an n-set. Let V be the 2^n-dimensional vector space (over some field $\mathcal{K}$) of all functions: $2^S \mapsto \mathcal{K}$. Let $\phi : V \mapsto V$ be the linear transformation defined by*

$$\phi f(T) = \sum_{Y \supseteq T} f(Y), \textit{for all } T \subseteq S.$$

Then ϕ^{-1} exists and is given by

$$\phi^{-1} f(T) = \sum_{Y \supseteq T} (-1)^{|Y-T|} f(Y), \textit{for all } T \subseteq S.$$

2 Main Results

We adopt the notation in [2]. For convenience, let $d(n, k) = \sum_{i=0}^{k} \binom{n}{i}$. Given $k < \lceil \frac{n}{2} \rceil$, for $\alpha \in \mathcal{F}_2^n$, let

$$\upsilon_k(\alpha) = (1, \alpha_1, \ldots, \alpha_n, \alpha_1\alpha_2, \ldots, \alpha_{n-1}\alpha_n, \ldots,$$

$$\alpha_1 \cdots \alpha_k, \ldots, \alpha_{n-k+1} \cdots \alpha_n) \in \mathcal{F}_2^{d(n,k)}$$

and $S_1(f)$ be the matrix with row vectors $\upsilon_k(\alpha)$ for all $\alpha \in 1_f$ and $S_0(f)$ be the matrix with row vectors $\upsilon_k(\beta)$ for all $\beta \in 0_f$. Here, row vectors are firstly ordered by their weight, secondly by lexicographical order. It's well known that f has algebraic immunity greater than k if and only if both row vectors in $S_1(f)$ and those $S_0(f)$ are two generating sets of $\mathcal{F}_2^{d(n,k)}$.

Rewrite $\upsilon_k(\alpha)$, $\alpha \in \mathcal{F}_2^n$ as follows,

$$\upsilon_k(\alpha) = \bigoplus_{\substack{\beta \preceq \alpha \\ \mathrm{wt}(\beta) \le k}} e_\beta, \tag{2}$$

where e_β is a vector in $\mathcal{F}_2^{d(n,k)}$ with one position 1 and the remainings 0 and $e_{\beta_1} \neq e_{\beta_2}$ if $\beta_1 \neq \beta_2$. Thus $\{e_\beta \mid \mathrm{wt}(\beta) \le k\}$ forms a basis of $\mathcal{F}_2^{d(n,k)}$. Using Mobious inversion, i.e., applying Lemma 1.1 with $\mathcal{K} = \mathcal{F}_2$ and vector $\alpha \in \mathcal{F}_2^n$ corresponding to a subset $\bigcup_{\alpha_i=0}\{s_i\}$ of an n-set $S = \{s_1, s_2, \ldots, s_n\}$, we have

$$e_\beta = \bigoplus_{\alpha \preceq \beta} (-1)^{\mathrm{wt}(\beta)-\mathrm{wt}(\alpha)} \upsilon_k(\alpha) = \bigoplus_{\alpha \preceq \beta} \upsilon_k(\alpha) \tag{3}$$

for $\mathrm{wt}(\beta) \le k$. Substituting (3) to (2) for those α with weight greater than k, we have

$$\begin{aligned}
\upsilon_k(\alpha) &= \bigoplus_{\substack{\beta \preceq \alpha \\ \mathrm{wt}(\beta) \le k}} e_\beta = \bigoplus_{\substack{\beta \preceq \alpha \\ \mathrm{wt}(\beta) \le k}} \bigoplus_{\gamma \preceq \beta} \upsilon_k(\gamma) \\
&= \bigoplus_{\substack{\gamma \preceq \alpha \\ \mathrm{wt}(\gamma) \le k}} \left(\upsilon_k(\gamma) \bigoplus_{\substack{\gamma \preceq \beta \preceq \alpha \\ \mathrm{wt}(\beta) \le k}} 1 \right) \\
&= \bigoplus_{\substack{\gamma \preceq \alpha \\ \mathrm{wt}(\gamma) \le k}} \upsilon_k(\gamma) \bigoplus_{\mathrm{wt}(\beta)=\mathrm{wt}(\gamma)}^{k} \begin{bmatrix} \mathrm{wt}(\alpha) - \mathrm{wt}(\gamma) \\ \mathrm{wt}(\beta) - \mathrm{wt}(\gamma) \end{bmatrix} \\
&= \bigoplus_{\substack{\gamma \preceq \alpha \\ \mathrm{wt}(\gamma) \le k}} \begin{bmatrix} \mathrm{wt}(\alpha) - \mathrm{wt}(\gamma) - 1 \\ k - \mathrm{wt}(\gamma) \end{bmatrix} \upsilon_k(\gamma).
\end{aligned} \tag{4}$$

The last step is valid, since $\begin{bmatrix} n \\ 0 \end{bmatrix} \oplus \begin{bmatrix} n \\ 1 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} n \\ m \end{bmatrix} = \begin{bmatrix} n-1 \\ m \end{bmatrix}$ holds for $n \ge 1$, $m \ge 0$, which can be easily proved by induction. Therefore, all $\upsilon_k(\alpha), \alpha \in \mathcal{F}_2^n$ can be explicitly represented as linear combinations of vectors $\upsilon_k(\alpha), \mathrm{wt}(\alpha) \le k$, which form a basis of $\mathcal{F}_2^{d(n,k)}$.

Denote by $S_{n,k}$ the $2^n \times d(n,k)$ matrix of which each row consists of the coefficients of the vector $\upsilon_k(\alpha)$ represented in basis $\{\upsilon_k(\beta) \mid \mathrm{wt}(\beta) \le k\}$. If the rows of $S_{n,k}$ are indexed by all vectors in $\mathcal{F}_2^n$ and the columns indexed by vectors with weight $\le k$, then

$$\begin{aligned}
& S_{n,k}(\alpha, \beta) \\
= & \begin{cases}
1, & \mathrm{wt}(\alpha) \le k \text{ and } \alpha = \beta, \\
1, & \mathrm{wt}(\alpha) > k,\ \beta \preceq \alpha \\
& \qquad \text{and } \begin{bmatrix} \mathrm{wt}(\alpha)-\mathrm{wt}(\beta)-1 \\ k-\mathrm{wt}(\beta) \end{bmatrix} = 1, \\
0, & \text{otherwise.}
\end{cases}
\end{aligned} \tag{5}$$

$$T_{15,7} = \left(\begin{array}{cccc|cc|cc} M_{8,0} & M_{8,1} & M_{8,2} & M_{8,3} & M_{8,4} & M_{8,5} & M_{8,6} & M_{8,7} \\ 0 & M_{9,1} & 0 & M_{9,3} & 0 & M_{9,5} & 0 & M_{9,7} \\ 0 & 0 & M_{10,2} & M_{10,3} & \multicolumn{2}{c|}{\multirow{2}{*}{0}} & M_{10,5} & M_{10,7} \\ 0 & 0 & 0 & M_{11,3} & & & 0 & M_{11,7} \\ \hline \multicolumn{4}{c|}{\multirow{4}{*}{0}} & M_{12,4} & M_{12,5} & M_{12,6} & M_{12,7} \\ & & & & 0 & M_{13,5} & 0 & M_{13,7} \\ & & & & 0 & 0 & M_{14,6} & M_{14,7} \\ & & & & 0 & 0 & 0 & M_{15,7} \end{array}\right).$$

Sometimes, it's suitable to write $S_{n,k}$ into partitioned matrices. Assume both row and column index vectors of $S_{n,k}$ are firstly ordered by their weight, secondly by lexicographical order. Then $S_{n,k} = \begin{pmatrix} I_{d(n,k)} \\ T_{n,k} \end{pmatrix}$ and $T_{n,k} \in \mathcal{F}_2(d(n,n-k) \times d(n,k))$ is partitioned into $(n-k) \times (k+1)$ submatrices, that is $T_{n,k} = (T_{ij})_{(n-k)\times(k+1)}$ and $T_{ij} = \begin{bmatrix} i-j+k \\ k-j+1 \end{bmatrix} M_{i+k,j-1}$. Here $M_{ij}(n)$ represents the $\binom{n}{i}$ by $\binom{n}{j}$ matrix of 0's and 1's whose rows are indexed by i-subsets I of an n-set X, whose columns are indexed by the j-subsets J of the same set X, and where the entry $M_{ij}(I,J)$ in row I and column J is 1 if $I \supseteq J$ and is 0 otherwise [4].

Theorem 2.1. *The number of Boolean functions f in $\mathcal{B}_n$ with algebraic immunity $k+1 \leq \lceil \frac{n}{2} \rceil$ and $|1_f| = d(n,k)$ equals the number of invertible submatrices in $T_{n,k} = (T_{ij})_{(n-k)\times(k+1)} \in \mathcal{F}_2(d(n,n-k) \times d(n,k))$, where $T_{ij} = \begin{bmatrix} i-j+k \\ k-j+1 \end{bmatrix} M_{i+k,j-1}$.*

Specifically, when $n = 2k+1$, the number of Boolean functions achieving maximum algebraic immunity is the number of invertible submatrices in $T_{n,k}$.

Proof. Since $S_{n,k} = (I_{d(n,k)}, T_{n,k})^T$, any set of $d(n,k)$ linearly independent rows in $S_{n,k}$ corresponds to an invertible matrix in $T_{n,k}$ [2], which means the number of Boolean functions having no annihilators with degree $\leq k$.

On the other hand, assume there exists $g \in \mathcal{B}_n$ such that $(f+1)g = 0$ and $0 < \deg(g) \leq k$, which implies $1_f \supseteq 1_g$. Taking an arbitrary $\beta \in 1_g$, define $1_{f'} = 1_f / \{\beta\}$. Since $|1_{f'}| < |1_f| = d(n,k)$, by solving $|1_{f'}|$ linear equations on $d(n,k)$ variables, we know there exists $0 \neq h \in \mathcal{B}_n$ such that $\deg(h) \leq k$ and $f'h = 0$, i.e, $1_f \subseteq 0_h \cup \{\beta\}$. Combining $1_g \subseteq 1_f \subseteq 0_h \cup \{\beta\}$, we have $1_h \cap 1_g = \{\beta\}$, i.e., hg takes 1 only at one point β, which is contradicted to $\deg(hg) \leq \deg(h) + \deg(g) \leq 2k < n$. Therefore, $f+1$ also has no annihilator with degree k or less.

When $n = 2k+1$, only balanced Boolean function can achieve maximum algebraic immunity [**?**], and thus the other part is proved. □

Example 2.2. *Let $n = 15$, $k = 7$. If f is the majority function in $\mathcal{B}_n$, then $S_1(f)S_0(f)^{-1} = T_{n,k}$, which is*

After knowing the explicit form of $S_{n,k}$, some counting results concerning algebraic immunity can be improved, such as the number of Boolean functions with maximum algebraic immunity in odd variables, which is proved to be not less than $2^{2^{n-1}}$ [2].

One possible way of counting or constructing all Boolean functions with maximum AI is to exchange some points in on-set with some in off-set of the majority function. With the explicit form of $S_{n,k}$, the following theorem concerns a simple situation that exchanging one point in 1_f with another in 0_f, where f is the majority function in odd number of variables.

Theorem 2.3. *There are exactly*

$$\sum_{\substack{i\wedge j=0\\ 0\le i,j\le k-1}} \binom{2k-1}{i+j+1 \quad k-i-1 \quad k-j-1} \tag{6}$$

Boolean functions in $\mathcal{B}_{2k-1}$ achieving maximum algebraic immunity by exchanging one point in 1_f with one point in 0_f, where f is the majority function in $\mathcal{B}_{2k-1}$.

Proof. It's clear that the number of such Boolean functions equals the number of the invertible one by one matrix, i.e., the number of 1's, in $S_1(f)S_0(f)^{-1} = T_{2k-1,k-1}$, where f is the majority function. Thus, let's count the number of 1's in the matrix $T_{2k-1,k-1}$. Firstly, the number of 1's in an arbitrary row in matrix $M_{i,j}$ is $\binom{i}{j}$, and thus there are $\binom{i}{j}\binom{2k-1}{i}$ number of 1's in $M_{i,j}$.

Since $T_{ij} = W_{i+k-1,j-1}(n)$ if $\begin{bmatrix} i-j+k-1 \\ k-j \end{bmatrix} = 1$, which is equivalent to $(k-j) \preceq (i-j+k-1)$, the total number of 1's in $T_{2k-1,k-1}$ is

$$\sum_{\substack{(k-j)\preceq(i-j+k-1)\\ 1\le i,j\le k}} \binom{2k-1}{i+k-1}\binom{i+k-1}{j-1}.$$

Replacing j in above equation by $k-j$ and replacing i by $i+1$, we have

$$\begin{aligned} &\sum_{\substack{j\preceq(i+j)\\ 0\le i,j\le k-1}} \binom{2k-1}{i+k}\binom{i+k}{k-1-j} \\ = &\sum_{\substack{j\preceq(i+j)\\ 0\le i,j\le k-1}} \binom{2k-1}{i+j+1 \quad k-i-1 \quad k-j-1}. \end{aligned}$$

Noting that $j \preceq (i+j)$ is equivalent to $i \wedge j = 0$, and the proof is complete. □

We can obtain similar counting result in even number of variables using the same method, of which the proof is omitted here.

Theorem 2.4. *There are exactly*

$$\sum_{\substack{i\wedge j=0\\ 0\le i<k\\ 0\le j\le k-1}} \binom{2k}{i+j+1 \quad k-i \quad k-j-1} \tag{7}$$

Boolean functions in $\mathcal{B}_{2k}$ achieving maximum algebraic immunity by exchanging one point in 1_f with one point in 0_f, where f is the majority function in $\mathcal{B}_{2k}$.

Due to the nice structure of $S_{n,k}$, a necessary condition only concerning the weight distribution of on-set and off-set for a Boolean function to achieve high algebraic immunity can be obtained.

Theorem 2.5. *Let $f \in \mathcal{B}_n$ be a Boolean function having no annihilator with degree $\leq k$. Then for any integers $0 \leq w_1 < w_2 < \cdots < w_m \leq k$, $m \geq 1$, we have*

$$\begin{aligned} &\sharp\{\alpha \in 1_f \mid wt(\alpha) = w_i \text{ or} \\ &\quad k - w_i \preceq wt(\alpha) - w_i - 1, 1 \leq i \leq m\} \\ \geq &\sum_{i=1}^{m} \binom{n}{w_i}. \end{aligned} \tag{8}$$

Proof. Using $\{\upsilon_k(\alpha) \mid \mathrm{wt}(\alpha) \leq k\}$ as a basis in $\mathcal{F}_2^{d(n,k)}$ instead of $\{e_\beta \mid \mathrm{wt}(\beta) \leq k\}$ to represent $\upsilon_k(\alpha)$, $\alpha \in \mathcal{F}_2^n$. And thus the $2^n \times d(n,k)$ coefficient matrix is $S_{n,k}$, which has an explicit form (5).

Since f has no annihilators with degree $\leq$ k, then there exists $d(n,k)$ vectors in 1_f, say $\alpha_1, \ldots, \alpha_{d(n,k)}$, such that $\upsilon_k(\alpha_1), \ldots, \upsilon_k(\alpha_{d(n,k)})$ are linearly independent, i.e., they form a basis of $\mathcal{F}_2^{d(n,k)}$. Taking the corresponding rows in matrix $S_{n,k}$, we obtain a square matrix with full rank $S'_{n,k}$. Denote the indexes of the columns in $S'_{n,k}$ corresponding to the vectors with weight equals some w_i by $j_1, \ldots, j_{\sum_{i=1}^m \binom{n}{w_i}}$. Since $S'_{n,k}$ has full rank, there exists integers $i_1, \ldots, i_{\sum_{i=1}^m \binom{n}{w_i}}$, such that $S'_{n,k}(i_1, \ldots, i_{\sum_{i=1}^m \binom{n}{w_i}}; j_1, \ldots, j_{\sum_{i=1}^m \binom{n}{w_i}})$ also has full rank, which implies in which there are no all-zero rows in this submatrix. Thus there are at least $\sum_{i=1}^m \binom{n}{w_i}$ vectors in 1_f corresponding to nonzero rows in $S_{n,k}(j_1, \ldots, j_{\sum_{i=1}^m \binom{n}{w_i}})$.

Now, let's count the vectors in 1_f corresponding to nonzero rows in submatrix $S_{n,k}(j_1, \ldots, j_{\sum_{i=1}^m \binom{n}{w_i}})$. According to (4), row α is nonzero if and only if $\mathrm{wt}(\alpha) = w_i$ or $\begin{bmatrix} \mathrm{wt}(\alpha) - w_i - 1 \\ k - w_i \end{bmatrix} = 1$ for some w_i. Therefore, there are

$$\begin{aligned} \sharp\{ \quad &\alpha \in 1_f \mid \mathrm{wt}(\alpha) = w_i \text{ or} \\ &k - w_i \preceq wt(\alpha) - w_i - 1, 1 \leq i \leq m\} \end{aligned}$$

nonzero rows, which should be not less than $\sum_{i=1}^m \binom{n}{w_i}$. □

Applying the last theorem to both f and $f+1$, we have the following corollary.

Corollary 2.6. *Let $f \in \mathcal{B}_n$ with algebraic immunity greater than k. Then for any integers $0 \leq w_1 < w_2 < \cdots < w_m \leq k$, $m \geq 1$, letting $I = \bigcup_{i=1}^m \{w_i\}$ and $J = \bigcup_{i=1}^m \{k+1 \leq w \leq n \mid k - w_i \preceq w - w_i - 1\}$, we have*

$$\sum_{i \in I} \binom{n}{i} \leq \sharp\{\alpha \in 1_f \mid wt(\alpha) \in I \cup J\} \leq \sum_{i \in J} \binom{n}{i}. \tag{9}$$

Here comes a question that is how to choose m numbers $w_1, w_2, \ldots, w_m$ to obtain a relatively strong necessary condition for algebraic immunity greater than k. Intuitively, the ratio of $\sum_{i \in J} \binom{n}{i}$ and $\sum_{i \in I} \binom{n}{i}$ should be close to 1.

Let $C(i) = \{k+1 \le w \le n \mid \begin{bmatrix} w-i-1 \\ k-i \end{bmatrix} = 1\}$, where $0 \le i \le k$. We claim

$$C(k-i) \supseteq C(k-i-p\cdot 2^{\lceil \log_2 (i+1)\rceil}) \tag{10}$$

for $p \in \mathbb{N}$. To prove (10), it's sufficient to show

$$\begin{bmatrix} w-(k-i)-1 \\ k-(k-i) \end{bmatrix} \ge \begin{bmatrix} w-(k-i-p\cdot 2^{\lceil \log_2 (i+1)\rceil})-1 \\ k-(k-i-p\cdot 2^{\lceil \log_2 (i+1)\rceil}) \end{bmatrix},$$

which is equivalent to

$$\begin{bmatrix} w' \\ i \end{bmatrix} \ge \begin{bmatrix} w'+p\cdot 2^{\lceil \log_2 (i+1)\rceil} \\ i+p\cdot 2^{\lceil \log_2 (i+1)\rceil} \end{bmatrix},$$

where $w' = w-k+i$. If $\begin{bmatrix} w' \\ i \end{bmatrix} = 1$, it's obvious. If $\begin{bmatrix} w' \\ i \end{bmatrix} = 0$, then

$$\begin{aligned} & \begin{bmatrix} w'+p\cdot 2^{\lceil \log_2 (i+1)\rceil} \\ i+p\cdot 2^{\lceil \log_2 (i+1)\rceil} \end{bmatrix} \\ = & \begin{bmatrix} w' \mod 2^{\lceil \log_2 (i+1)\rceil} \\ i \mod 2^{\lceil \log_2 (i+1)\rceil} \end{bmatrix} \begin{bmatrix} \lfloor \frac{w'}{2^{\lceil \log_2 (i+1)\rceil}} \rfloor + p \\ \lfloor \frac{i}{2^{\lceil \log_2 (i+1)\rceil}} \rfloor + p \end{bmatrix} \\ \le & \begin{bmatrix} w' \mod 2^{\lceil \log_2 (i+1)\rceil} \\ i \mod 2^{\lceil \log_2 (i+1)\rceil} \end{bmatrix} \\ = & \begin{bmatrix} w' \mod 2^{\lceil \log_2 (i+1)\rceil} \\ i \end{bmatrix} \\ \le & \begin{bmatrix} w' \\ i \end{bmatrix} = 0. \end{aligned}$$

Therefore, if number i is taken as one of $w_1, w_2, \ldots$, it's wise to take numbers $i - p\cdot 2^{\lceil \log_2 (i+1)\rceil}$, $p = 1, 2, \ldots$, as well.

Example 2.7. *According to* (10)*, we use the following strategy to choose w_i's step by step. First, choosing $k-1-2p$, $p = 0, 1, \ldots$, we obtain a necessary condition. Secondly, adding $k-2-2^2p$, $p = 0, 1, \ldots$, we obtain another necessary condition. In the step t, adding $k - 2^{t-1} - 2^t p$, $p = 0, 1, \ldots$, we can obtain a necessary condition. It's worth noticing that $\{k - 2^{t-1} - 2^t p \mid p \in \mathbb{N}\}$, $t = 1, 2, \ldots, \lfloor \log_2 k \rfloor + 1$ is a decomposition of $\{0, 1, \ldots, k-1\}$, i.e., they are pairwise unintersected and their union is $\{0, 1, \ldots, k-1\}$. We demonstrate this strategy for $n = 15$, $k = 7$ as follows.*

- *Let $m = 4$, $w_1 = 6, w_2 = 4, w_3 = 2, w_4 = 0$. Thus $I = \{0, 2, 4, 6\}$, $J = \{8, 10, 12, 14\}$ and the necessary condition is*

$$6476 \le \sharp\{\alpha \in 1_f \mid wt(\alpha) \in I \cup J\} \le 9908.$$

- *Let $m = 6$, adding $w_5 = 5$, $w_6 = 1$. Thus $I = \{0, 1, 2, 4, 5, 6\}$, $J = \{8, 9, 10, 12, 13, 14\}$ and the necessary condition is*

$$9494 \le \sharp\{\alpha \in 1_f \mid wt(\alpha) \in I \cup J\} \le 15018.$$

- *Let $m = 7$, adding $w_7 = 3$. Thus $I = \{0, 1, 2, 3, 4, 5, 6\}$, $J = \{8, 9, 10, 11, 12, 13, 14\}$ and the necessary condition is*

$$9949 \leq \sharp\{\alpha \in 1_f \mid wt(\alpha) \in I \cup J\} \leq 16383.$$

References

[1] R. P. Stanley, *"Enumerative Combinatorics, Volumn I,"* Cambridge University Press, 1997.

[2] N. Li, L. Qu, W. Qi, G. Feng, C. Li and D. Xie, *"On the construction of Boolean functions with optimal algebraic immunity,"* IEEE Trans. on Information Theory, vol.54, no.3, pp.1330-1334, MARCH 2008.

[3] A. Canteaut, *"Open problems related to algebraic attacks on stream ciphers,"* in Proc. WCC 2005, Invited talk, pp.1-10.

[4] R. M. Wilson, *"A diagonal form for the incidence matrices of t-subsets vs k-subsets,"* Eur. J. Combin., vol. 11, pp. 609-614, 1990.

[5] C. Carlet, D. K. Dalai, K. C. Gupta, and S. Maitra, *Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction,* IEEE Trans. Inf. Theory, vol.52, no.7, pp.3105-3121, Jul.2006.

[6] F. Armknecht., *"Improving fast algebraic attacks"*, In FSE 2004, vol.3017 of Lecture Notes in Computer Science, pp.65-82, Spring-Verlag, 2004.

[7] L. Qu, K. Feng, F. Liu, and L. Wang, *"Constructing symmetric Boolean function with maximum algebraic immunity"*, IEEE Trans. on Information Theory, vol.55, no.5, pp.2406-2412, MAY, 2009.

[8] D. K. Dalai, S. Maitra, and S. Sarkar, *"Basic theory in construction of Boolean functions with maximum possible annihilator immunity,"* Des. Codes, Cryptogr., vol.40, no.1, pp.41-58, 2006.

[9] N. Courtois, *"Fast algebraic attacks on stream ciphers with linear feedback,"* in Advances in Crypltology—CRYPTO 2003 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2003, vol. 2729, pp. 176C194.

[10] R. L. Graham, D. .E. Knuth and O. Patashnik, Concrete Mathematics: A Foundation for Computer Science, 2nd Edition, Pearson Education, 1994.

[11] A. Canteaut and M. Videau, *"Symmetric Boolean functions"*, IEEE Trans. on Information Theory, vol.51, no.8, pp.2791-2811, Aug., 2005.

[12] A. Braeken, *"Cryptographic Properties of Boolean functions and S-Boxes"*, thesis, Mar., 2006.